e-ISSN **3041-2498**

Public Management and Policy

https://www.eu-scientists.com/index.php/pmap

International security system in the light of cyber threats: Legal issues and prospects

Sergii Troshchenkov [1] ● Inesa Halona [2]

[1] *Citibank Europe PLC (Poland). Vice President in Scenario Design, PhD in Economics and Quantitative Methods.*

[2] *National Transport University (Ukraine). Associate Professor at the Department of Transport Technologies, PhD in Engineering, PhD in Law, Associate Professor.*

*** *Corresponding Author,*** e-mail: sergii.troshchenkov@gmail.com

ARTICLE INFO

Research Article

Received:
1 August 2024
Revised:
4 September 2024
Accepted:
17 September 2024
Published online:
30 September 2024

DOI: 10.70651/3041-2498/2024.1.07

ABSTRACT

The study is devoted to systematizing the problems related to cybersecurity in the context of rapid technological development and globalization of the digital space, as well as to finding effective solutions to these problems. The purpose of the study is to identify the main challenges faced by states, organizations and individuals in the field of cybersecurity, as well as to develop recommendations for improving legal and organizational mechanisms for responding to cyber threats. The results of the study, based on the analysis of critical literature and the application of methods of analysis, synthesis, grouping, comparative analysis and modeling, demonstrate a comprehensive understanding of the key challenges in the field of cybersecurity. It is established that the rapid development of technology requires continuous updating of the legal framework to meet modern technological realities, but legislative bodies often fail to adapt to these changes. In addition, significant differences in technological development between countries create unequal opportunities for the protection of information systems at the national level. The problem of incompatibility and inconsistency of international and national norms governing cyberspace leads to legal conflicts and complicates the formation of an effective protection mechanism. A final challenge is defining responsibility and ethical boundaries in cyberspace, which requires international consensus and clear legal definitions. Addressing these challenges requires an integrated approach that includes adapting legal structures to rapid changes in technology, strengthening international cooperation to bridge the technological development gap, harmonizing international and national cybersecurity standards, and clearly delineating responsibilities and establishing ethical boundaries in cyberspace. Such an approach will help ensure sustainability and security in the digital world, adapting to the unpredictable challenges of our time. The practical significance of this study is that it suggests ways to improve the effectiveness of protecting information systems and infrastructures in the face of global cyber threats, which will contribute to ensuring stability and security at the international level. It points to the importance of coordinated interaction between states, academia and the private sector in developing and implementing comprehensive cybersecurity strategies adapted to modern challenges.

KEYWORDS

Cybersecurity, international protection system, legal regulation, liability.

e-ISSN **3041-2498**

Публічне управління і політика

https://www.eu-scientists.com/index.php/pmap

Система міжнародної безпеки у світлі кіберзагроз: правові проблеми та перспективи

Сергій О. Трощенков [1]* • Інеса І. Гальона [2]

[1] *Сітібанк Європа (Польща). Віце-президент з розробки сценаріїв, доктор філософії з економічних наук та кількісних методів.*

[2] *Національний транспортний університет (Україна). Доцент кафедри транспортних технологій, к. т. н., к. ю. н., доцент.*

*** *Автор-кореспондент,*** e-mail: sergii.troshchenkov@gmail.com

СТАТТЯ

Дослідницька

отримана:
1 серпня 2024 р.
переглянута:
4 вересня 2024 р.
прийнята:
17 вересня 2024 р.
опублікована онлайн:
30 вересня 2024 р.

DOI: 10.70651/3041-2498/2024.1.07

АНОТАЦІЯ

Дослідження присвячене систематизації проблем, пов'язаних із забезпеченням кібербезпеки у контексті швидкого розвитку технологій та глобалізації цифрового простору, а також пошуку ефективних рішень для цих проблем. Мета дослідження полягає в ідентифікації основних викликів, з якими стикаються держави, організації та індивіди у сфері кібербезпеки, а також у розробці рекомендацій щодо вдосконалення правових та організаційних механізмів реагування на кіберзагрози. Результати дослідження, що базуються на аналізі критичної літератури та застосуванні методів аналізу, синтезу, групування, порівняльного аналізу та моделювання, демонструють комплексне розуміння ключових викликів у сфері кібербезпеки. Встановлено, що стрімкий розвиток технологій вимагає невпинного оновлення правових рамок, щоб вони відповідали сучасним технологічним реаліям, але законодавчі органи часто не встигають адаптуватися до цих змін. Крім того, значні розбіжності у технологічному розвитку між країнами створюють нерівні можливості для захисту інформаційних систем на національному рівні. Проблема несумісності та неузгодженості міжнародних та національних норм, що регулюють кіберпростір, призводить до юридичних колізій та ускладнює формування ефективного механізму захисту. Останнім викликом є визначення відповідальності та етичних меж в кіберпросторі, що вимагає міжнародного консенсусу та чітких правових визначень. Вирішення цих проблем потребує інтегрованого підходу, який включає адаптацію правових структур до швидких змін в технологіях, посилення міжнародної співпраці для усунення розриву в технологічному розвитку, гармонізацію міжнародних і національних стандартів кібербезпеки, а також чітке розмежування відповідальності та встановлення етичних рамок у кіберпросторі. Такий підхід дозволить забезпечити стійкість та безпеку в цифровому світі, адаптуючись до непередбачуваних викликів сучасності. Практичне значення цього дослідження полягає в тому, що воно пропонує шляхи підвищення ефективності захисту інформаційних систем та інфраструктур в умовах глобальних кіберзагроз, що сприятиме забезпеченню стабільності та безпеки на міжнародному рівні. Воно вказує на важливість злагодженої взаємодії між державами, науковою спільнотою та приватним сектором у розробці та імплементації комплексних стратегій кібербезпеки, що адаптовані до сучасних викликів.

КЛЮЧОВІ СЛОВА

кібербезпека, міжнародна система захисту, правове регулювання, відповідальність.

1. Introduction

In today's world, where globalization and digitalization penetrate every aspect of our lives, international security is acquiring a new dimension in the context of cyber threats. These threats, which recognize no borders, can impact not only the national security of countries but also the safety and well-being of individuals. The relevance of cyber threats is underscored by their ability to disrupt peace and stability, affecting critical infrastructures, financial systems, and the private lives of citizens.

The United Nations (UN) acknowledges the importance of cybersecurity in maintaining international peace and security and is actively engaged in developing and implementing policies and initiatives in this field. Despite this, the continuous evolution of cyber threats requires each country and individual to be prepared to detect, prevent, and respond to potential incidents.

Given these circumstances, the topic of cybersecurity becomes particularly pertinent. It reflects the need for a thorough analysis of existing legal frameworks, identification of their weaknesses, and the development of effective international mechanisms capable of adequately responding to the challenges of the modern cyberspace.

2. Literature Review

The issue of international security in the context of cyber threats and legal aspects is extensively covered in academic research, highlighting global interest and the significance of this issue. A notable contribution to the understanding of this topic is made by O. Hathaway et al. (2012), who thoroughly analyze the legal aspects of cyber-attacks, pointing out the difficulties in applying existing norms of international law to cyberspace [1]. Another important study by I. Duic, V. Cvrtila and T. Ivanjko examines the contemporary challenges to international cybersecurity and the need for the development of effective intergovernmental response mechanisms to cyber threats [2].

In the realm of legal issues, I. Ivory (2023) highlights the latest developments in cybersecurity and the associated legal challenges, emphasizing the importance of adapting legislation to the rapidly changing digital environment [3]. Additionally, Y. Kotukh (2020) showcases the process of forming cybersecurity systems at the governmental level, underscoring the significance of an institutional approach in ensuring national security in cyberspace [4].

Materials from leading expert organizations and online publications, including works by the Observer Research Foundation (2022) and the World Economic Forum report (2024), were also utilized in the research [5; 6]. These sources shed light on current trends and the future of international law in cyberspace.

Despite the extensive body of literature on this topic, there remains a need for a systematic analysis that encompasses various aspects of international cybersecurity. This will not only provide a deeper understanding of existing challenges but also help develop more effective strategies for overcoming them at the international level.

3. Problem Statement

The purpose of the study is to identify the main challenges faced by states, organizations and individuals in the field of cybersecurity, as well as to develop recommendations for improving legal and organizational mechanisms for responding to cyber threats.

4. Methods and Materials

In analyzing critical literature, both academic and expert, a variety of issues in the cybersecurity sphere were examined. Each source contributes to the understanding of specific aspects of the issue, facilitating the systematization and grouping of information. This approach led to the development of a problem classification across four main areas, encompassing a broad range of challenges from technological gaps to international coordination and legal matters. The application of inductive and deductive methods allowed for a deeper analysis of the collected data, modeling various scenarios, and identifying potential solution directions. The focus was on developing strategies to enhance cybersecurity levels, particularly through improving the legal framework, strengthening international

cooperation, adapting to the rapidly changing technological environment, and considering ethical aspects in cyberspace.

5. Results and Discussion

In the realm of cybersecurity, legal challenges are particularly pressing and complex due to the rapid pace of technological development and the globalization of the digital space [7]. One of the main issues is the rapid advancement of new technologies, leading to the emergence of new types of cyber threats [6]. This necessitates continuous updates to legal frameworks and response mechanisms, often outpacing the ability of legislative bodies to adapt to innovations. A second issue is the significant disparity in technological development between countries, complicating the creation of uniform cybersecurity standards suitable for all international actors [8]. This disparity leads to unequal capabilities among countries to protect their information systems and infrastructure from cyberattacks. A third issue is the incompatibility of international documents and norms governing cyberspace. Different approaches to cybersecurity, adopted at various levels (international, regional, and national), may contradict each other or be insufficiently coordinated, complicating the creation of an effective and unified defense system [1; 4; 5].

The issues of responsibility and ethics in cyberspace remain contentious. Determining responsibility for cyber incidents, as well as delineating the ethical boundaries of cyber operations, requires clear legal definitions and international consensus, which is a challenging task amidst the constantly evolving technological landscape and international relations [3].

The emergence of new technologies, such as artificial intelligence, is part of the changing landscape of international relations and their legal basis, potentially leading to a reassessment of the international security system with the continuous introduction of new technologies. Among the new challenges presented by cyber technologies are old challenges: the use of technologies for hostile actions and acts of aggression, interference in civilian infrastructure, destabilization of socio-political situations, dissemination of false information, and the destruction or blocking of computer systems and networks. New forms of cyberattacks have also emerged, utilizing deepfake technologies and manipulation of consciousness. Today, with the development of artificial intelligence, cyber threats are increasing worldwide. According to a 2024 survey of business owners, with the implementation of artificial intelligence technologies into various software, businesses are most concerned about the mass leakage of data (46%). 20% of respondents are worried about the disclosure of private information, and 8% are concerned about the breach of commercial secrets and the theft of intellectual property [6].

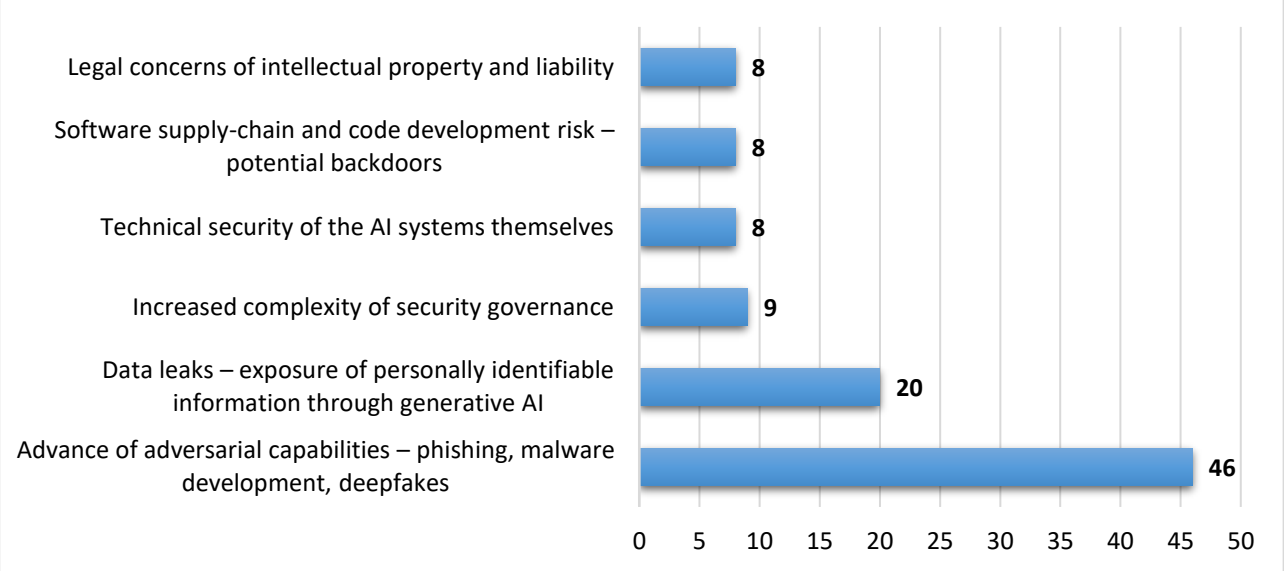

Figure 1. The level of various types of cyber threats to business

Source: Compiled by the author based on data from WEF [6].

Given The challenges of legal regulation in the context of artificial intelligence (AI) and cyber technologies are deeply rooted and are due to the dynamic development of technologies that significantly outpace the legal system's ability to adapt to new challenges. The main issues include:

– Deficiencies in legislation: existing legislation often fails to account for the specifics of AI and cyber technologies, leading to legal gaps in the regulation of these areas. In particular, there arises the issue of liability for actions conducted through AI, including cyber-attacks, data breaches, and other negative consequences.

– Technical challenges: the rapid development of technologies complicates accurate forecasting and understanding of the potential consequences of their application, making it difficult to introduce adequate changes to the legislation.

The prospects for the development of legal regulation of AI and cyber technologies are determined by the following directions:

– Adaptive legislation: Developing flexible legal norms that can adapt to the rapid development of technologies while ensuring the protection of human rights and freedoms.

– Engagement of experts: Collaboration with technical specialists and scientists to ensure a deep understanding of technologies in the formation of legislative initiatives.

– Ethical frameworks: Establishing ethical principles for the development and use of AI, which will promote the creation of safe and responsible artificial intelligence.

The development of legal regulation in this area requires a balanced approach that combines the protection of human rights, economic interests, and security, taking into account the potential and risks associated with new technologies.

The diverse technological development levels of countries significantly influence the transformation of international security and the very concept of security itself. The new cyber dimension of international relations presents a serious challenge to the theories of maintaining each country's power. Today, cybersecurity is on par with national security for every country, which is not surprising given the gradual shift of all administrative and economic processes to digital technologies. Each country has unique features in the context of cybersecurity that affect its ability to repel cyberattacks, protect its networks, and even conduct offensive cyber operations. Scholars I. Duic, V. Cvrtila an T. Ivanjko identify three key factors that shape national cyber power [2]:

– Offensive cyber capabilities;
– National dependency on cyber networks;
– The ability of a country to defend and control its cyberspace.

Table 1. The level of cybersecurity of some countries in the world in terms of protection policy and dependency on cyber threats

Nation	Dependency on the Cyber Network	Defensive Capabilities
USA	Low	Low
Russia	Middle	Middle
China	Middle	Middle
Iran	Middle	Low
North Korea	High	High

Given the unique level of protection and cybersecurity policy of each country, there's a clear challenge related to legal regulation of cybersecurity at the international level. The primary obstacle is that a single comprehensive legal mechanism cannot adequately account for all these unique features, thus potentially compromising the interests and security aspects of individual countries. For instance, the United States is characterized as a country with a low dependency of administrative and economic systems on cyber threats and a low level of defensibility, whereas North Korea has a high dependency on cyber networks and a high level of defensibility.

These differences are key when considering international legal regulation of cybersecurity, as any general laws or treaties need flexibility to accommodate these unique aspects. The inability to create a single regulatory standard that effectively addresses the needs of all countries leads to the search for alternative cooperation methods, such as regional agreements or bilateral arrangements, which can be more flexible and adaptable to the specific needs and capabilities of each country.

The prospects for resolving legal regulatory issues related to the varying levels of technical and technological development of countries include the following approaches and strategies:

– Development of flexible international frameworks: creating multi-level international agreements that provide basic principles and standards for all countries, as well as allowing for regional

and local adaptations. This could include flexibility in the implementation of standards, depending on the technical level and specific needs of each country.

– Strengthening international cooperation: enhancing international cooperation through joint research projects, the exchange of knowledge and best practices in cybersecurity, and the development of joint training and professional development programs.

– Formation of joint research initiatives: establishing international research groups to study cybersecurity features in different cultural, economic, and technological conditions. This will allow for a better understanding of the specificity of cyber threats and the development of targeted protection strategies.

– Utilization of mutual assistance mechanisms: developing mechanisms for mutual assistance and support between countries, especially in situations of cyber crises and incidents that require rapid intervention and the pooling of resources for an effective response.

By implementing these prospects, greater unification of legal regulation of cybersecurity can be achieved, taking into account the different levels of technical and technological development of countries, and ensuring adequate protection against cyber threats at the global level.

Unsystematic regulatory framework. The normative legal base structures cybersecurity and creates a certain imperative environment in cyberspace. This dimension is aimed at forming a national cyber ecosystem through the creation of norms and standards, as well as law enforcement, related to government or organizational actions to reduce cyber threats or repel cyber attacks. The main issues with legal regulation include the fact that international and national documents regulating cybersecurity consist of a set of outdated, new, duplicative, and country-specific laws.

Active development and implementation of cybersecurity systems (CSS) at various levels have been noted since the early 2000s. The general principles and main features of these systems are reflected in a number of key documents that define approaches and standards in this area at the international level. Table 2 shows the main guiding documents developed by various organizations and institutes.

Based on the study [4], the issue of adopting common cybersecurity laws at the international level is quite complex due to different approaches and interests of countries. Examining the normative documents of recent years, particularly the report of the United Nations Open Working Group (OEWG), reveals that France supports the effective implementation of already agreed norms and principles in cyberspace. In contrast, the United States, in its comments on the draft OEWG report, is even more categorically against creating new normative concepts, considering it a futile effort. On the other hand, China, in its contribution, criticizes the report's stance that "existing international law, supplemented by voluntary non-binding norms reflecting consensus among states, is currently sufficient," arguing that new realities should be shaped by new normative mechanisms for a more "favorable" international response.

Furthermore, contributions from the European Union, France, the USA, and Australia confirm the applicability of international humanitarian and human rights law to cyber operations. However, such positions encounter significant resistance from countries like Iran, China, Russia, and Cuba, whose contributions argue that applying international humanitarian law (IHL) will lead to unnecessary militarization of cyberspace. These differences significantly impacted the breakdown of negotiations during the fifth Group of Governmental Experts (GGE) in 2017, resulting in Cuba, China, and Russia leaving the discussions and, consequently, not accepting the report based on consensus.

The discussion around including the phrase "Public Core" in the final OEWG report is noteworthy. Although not widely spread, it is interesting in the context of the second principle of the non-binding Paris Call for Trust and Security in Cyberspace adopted in 2018, and commitments to preserving the accessibility and integrity of the Internet during GGE and OEWG discussions. Countries like the Netherlands, the USA, and France promote the concept of protecting the "public core of the Internet," i.e., the protocols and software infrastructure that make the Internet a "global common good," whereas China rejects their relevance, asserting that concepts like the "Public Core" have not yet received global consensus.

Particularly deserving of attention is the issue of attribution and state responsibility. According to the 2001 Draft Articles of the International Law Commission on the Responsibility of States for Internationally Wrongful Acts, attributing a crime committed under international law to a state is essential for applying the principle of state responsibility. While the draft articles themselves are non-binding, the duo of attribution and state responsibility is recognized as customary law. The discussion

revolves around whether there should be common norms for attribution and dispute resolution regarding wrongful acts in cyberspace, as is the case for other conventional crimes and wrongful acts, or whether the sovereignty of the state and the diplomatic right to make a national decision on attribution should prevail over a common approach [5].

Table 2. Chronological presentation of major global normative cybersecurity documents

System	Guiding Documents (Years)
Cybersecurity Strategy of the Organization of American States (OAS)	Comprehensive Inter-American Cybersecurity Strategy: A Multifaceted and Multidisciplinary Approach to Creating a Culture of Cybersecurity (2004)
Global Cybersecurity Agenda (ITU-GCA)	Report of the Chairman of the High-Level Expert Group (HLEG) on the Global Cybersecurity Agenda (GCA) of ITU (2007, 2012, 2014) National Cybersecurity Strategy Guide Global Cybersecurity Index (GCI)
Framework of the Business Software Alliance (BSA)	BSA Global Cybersecurity System (2010)
Principles and Guidelines of the World Economic Forum (WEF)	Partnership for Cyber Resilience: Risk and Responsibility in a Hyperconnected World (2012, 2016) Principles and Guidelines Risk and Responsibility in a Hyperconnected World: Paths to Global Cyber Resilience Risk and Responsibility in a Hyperconnected World: Implications for Enterprises
Guidance from the Cooperative Cyber Defence Centre of Excellence (CCDCOE)	Guidance on National Cybersecurity System (2012)
ISO 27032	Information technology – Security techniques – Guidelines for cybersecurity (ISO/IEC 2012)
EU Cybersecurity Strategy	National Cybersecurity Strategies: Practical Guide on Development and Execution (ENISA 2012a) EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace
Cybersecurity Guidance from Microsoft	Developing a National Cybersecurity Strategy: Fundamentals, Security, Growth, and Innovation (2013)
ISACA's Nexus for Cybersecurity	Transforming Cybersecurity (2013)
System of the National Institute of Standards and Technology (NIST)	Framework for Improving Critical Infrastructure Cybersecurity (2013)
Cybersecurity Capability Maturity Model (CMM)	Cybersecurity Capability Maturity Model (2014)
Cybersecurity Guidelines of the Commonwealth	Commonwealth Approach to Developing National Cybersecurity Strategies: A Guide to Creating Comprehensive and Inclusive Approaches to a Safe, Secure, and Resilient Cyberspace (CTO 2015) Commonwealth Cyber Governance Model
UN Open Working Group (OEWG)	Formation of International Norms and Principles in Cybersecurity (2015)
Group of Governmental Experts (GGE)	Recommendations on the Application of International Law, Norms of Behavior, as well as Measures to Strengthen Trust and Cooperation in Cyberspace (2021).
EU Directive ("NIS 2")	Introduces regulations for non-compliance with cybersecurity (2022)

Source: Systematized by the author on the basis of Y. Kotukh [4].

Developing a legal basis to address the issues of the non-systemic and inconsistent legislative base among themselves and between countries' interests requires a comprehensive approach that considers both the need for unification and harmonization of standards and the necessity to preserve national sovereignty and the specificity of each country. For this, the following development perspectives can be considered:

– Harmonization of international standards: development of unified international standards and regulations that would consider the basic requirements for cybersecurity and privacy, which could serve as a foundation for national legislations. This could simplify interactions between countries and reduce inconsistency issues.

– International agreements and conventions: conclusion of international agreements that provide legal frameworks for cooperation in the field of cybersecurity, including issues of cyber attack

attribution and liability for violations. Such agreements could also include mechanisms for dispute resolution and sanctions for violations.

– Cooperation with the private sector: involvement of companies and private sector experts in the process of forming the legal base to ensure consideration of practical experience and current technological trends.

– Interdisciplinary approach: combination of legal, technological, economic, and social analysis in the development of legislation to ensure a comprehensive approach to cybersecurity.

– Awareness raising and educational programs: development and implementation of programs to raise awareness among legislators, public officials, and the public about the importance and complexities of cybersecurity.

– Strengthening international jurisdiction: development of international legal institutions capable of handling cases related to cybercrime and international cybersecurity, which could contribute to more effective resolution of transnational conflicts.

– Technical assistance and support to developing countries: provision of technical assistance and support to developing countries to build their national cyber defense and integrate into the international cybersecurity system.

Applying these perspectives requires joint efforts of the international community, national governments, the private sector, and civil society to achieve greater consistency and effectiveness in the legal regulation of cybersecurity at the global level.

Regarding Cybersecurity Accountability. In the context of combating cyber threats at both national and corporate levels, the European Union has recently adopted Directive (EU) 2022/2555 ("NIS 2"), aiming to enhance the overall cybersecurity level across a broad array of organizations operating within the EU. This includes sectors such as energy, transport, water supply, banking, financial market infrastructures, healthcare, digital infrastructure, and digital services. NIS 2 introduces a series of cybersecurity obligations, including those related to organizational governance, operational risk management, and incident reporting. Each EU Member State is required to implement laws within their jurisdiction to operationalize NIS 2 by October 17, 2024. Companies operating across different jurisdictions must be familiar with the cybersecurity laws applicable to their activities. Specifically, companies should understand their obligations in developing cybersecurity breach response strategies and cybersecurity risk management systems, as well as the impact of specific country laws on these systems (e.g., the legality of "ethical hacking" services), and the reporting obligations that arise following a cybersecurity breach [3].

The legal and administrative consequences of cybersecurity breaches can be severe for affected companies, ranging from significant fines and regulatory sanctions, government audits, lengthy regulatory investigations, and even criminal liability. The disruption of business operations and the loss of data, intellectual property, and confidential information can also be costly in terms of financial losses, market position, and rectification expenses. Perhaps more importantly, companies experiencing cybersecurity breaches become the focus of negative media attention and immeasurable damage from the loss of consumer trust [3].

Companies also face the threat of legal actions from customers, employees, and business partners, especially if these groups claim to have incurred actual financial losses. In the US, there have been instances where shareholders have filed class action lawsuits against companies when announced cybersecurity breaches led to a drop in the company's stock price, allegedly due to inadequate security measures taken [3].

While lawsuits and regulatory actions are typically directed at the company that suffered the cybersecurity breach, directors and officers are the primary individuals held accountable for failing to take steps to mitigate or eliminate cyber threats. In the US, direct legal actions have been initiated against company directors, including by the Department of Justice and the Federal Trade Commission, in response to the management of a cybersecurity breach, its reporting, and the potential inability to protect customer personal information [3].

It is entirely possible that European authorities will decide to hold directors personally accountable and subject to regulatory censure as a result of managerial mistakes that led to a cyberattack or (equally importantly) to subsequent mishandling of the cybersecurity breach or failure to report it. In particular, the aforementioned NIS 2 Directive recently introduced in the EU requires that laws adopted in each EU Member State obligate the governing bodies of relevant organizations to review

the cybersecurity risk management measures implemented to comply with NIS 2 requirements and to oversee the execution of these measures.

To reduce the level of risk, companies should develop policies and recognized standards, including those related to incident response, data security, and data retention, as well as robust employee training and monitoring programs. This should also comply with best practices for authenticating and authorizing remote workers to limit unwarranted access to software, files, and the company's intranet (which may involve engaging third-party authentication services). This should be combined with appropriate governance structures and processes. Contracts with employees, suppliers, and third parties should include relevant provisions on issues such as security standards, data access, management and control, and liability. Adequate cybersecurity insurance with sufficient coverage for incident response and mitigation, breach notification, outages, and business-level damages, as well as related legal issues such as regulatory fines and additional consulting costs, should be carefully considered. Any exclusions from the insurance policy should be thoroughly reviewed [3]

The development of legislation regarding cybersecurity accountability focuses on ensuring a proper balance between the protection of consumers, data, and infrastructure on the one hand, and the responsibilities and obligations of companies on the other. The evolution of legislation in this field aims to make organizations more accountable for protecting the data and systems they use and manage. The main directions for the development of accountability issues are through:

– Establishing clear incident response procedures: legislation defines clear procedures and timelines for responding to cybersecurity incidents and for reporting such incidents to the relevant regulatory authorities and affected parties.

– Personal accountability of management: an increasing trend towards holding organizational leaders personally accountable for ineffective cybersecurity management and inadequate data protection measures.

– Cooperation between the state and private sector: legislation should facilitate and regulate cooperation between government agencies and the private sector for the exchange of information about cyber threats and best cybersecurity practices.

– Consumer rights protection: enhancing the accountability of organizations for maintaining and protecting consumers' personal data and ensuring their right to know how their information is used.

Overall, the prospects for the development of legal regulation of international cybersecurity encompass a broad range of aspects, including the adaptation of existing mechanisms and the development of new tools and institutions specifically designed to respond to cyber threats. One of the main challenges is the inefficiency of many existing international institutions and mechanisms in the field of cybersecurity, necessitating changes both at the level of tools and approaches to international security [9].

Instrumental Changes: instrumental changes involve reorganizing existing security mechanisms and developing new tools for adequately responding to modern cyber threats. This may include establishing clear incident response procedures, cooperation between the state and the private sector, international agreements and conventions, strengthening international jurisdiction, providing technical assistance and support to developing countries, developing flexible international frameworks, enhancing international cooperation, forming joint research initiatives, utilizing mutual assistance mechanisms, adaptive legislation, engaging experts to address issues, and more.

Conceptual Changes: conceptual changes refer to the reconsideration of fundamental approaches to international security in the context of cyberspace. This includes the choice between protecting national security within one's own borders and actively participating in the global information order to collectively counter cyber threats. Given the transnational nature of cyberspace, conceptual changes consider personal accountability of leadership, consumer rights protection, harmonization of international standards, an interdisciplinary approach to problem-solving, increased awareness and educational programs, ethical frameworks of responsibility, understanding the need for international cooperation, and the development of joint defense strategies that involve both governmental and private structures for effective cybersecurity provision [10].

Both areas of change require a comprehensive approach that combines technical, legal, and strategic aspects of international cybersecurity. Considering the rapid development of technologies and the continuous evolution of cyber threats, the international community must dynamically adapt to new challenges by developing and implementing effective protection mechanisms in cyberspace.

6. Conclusions

The analysis of cybersecurity issues has revealed four key challenges. The first is the rapid progress in technologies, which generates novel types of threats. This dynamic requires continuous updating of legal norms and responses, but legislative bodies often struggle to keep up with the pace of changes in the technological world. The second issue lies in the significant disparities in technological development among countries, complicating the formation of universal cybersecurity standards acceptable to all. This creates a difference in the capabilities of states to protect their information systems. The third aspect is the incompatibility and inconsistency between international and national norms regulating cyberspace, leading to legal fragmentation and complicating the creation of an effective protection mechanism. Finally, the fourth problem is the issue of accountability and ethical boundaries in cyberspace, where it is necessary to clearly define who is responsible for what, especially in the context of the constantly changing technological landscape. Addressing the identified cybersecurity problems requires a comprehensive approach that includes adapting legal frameworks to the rapidly changing technological environment, international cooperation to align technological development, unification of international and national cybersecurity norms, and clear definition of accountability and ethical boundaries in cyberspace.

References

1. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review, 100*(4), 817–885. https://openyls.law.yale.edu/bitstream/handle/20.500.13051/3283/Law_of_Cyber.pdf
2. Duic, I., Cvrtila, V., & Ivanjko, T. (2017). *International cyber security challenges*. 1309–1313. https://doi.org/10.23919/MIPRO.2017.7973625
3. Ivory, I. (2023). Cybersecurity developments and legal issues. *White & Case*. https://www.whitecase.com/insight-alert/cybersecurity-developments-and-legal-issues
4. Kotukh, Y. V. (2020). Formuvannia system kiberbezpeky v orhanakh publichnoi vlady [Formation of cybersecurity systems in public authorities]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, (3). http://www.dy.nayka.com.ua/pdf/3_2020/32.pdf (in Ukrainian)
5. Observer Research Foundation. (2022). The near future of international law in cyberspace: Contentions and realities. https://www.orfonline.org/expert-speak/the-near-future-of-international-law-in-cyberspace-contentions-and-realities
6. World Economic Forum (2024). Global cybersecurity outlook 2024. http://surl.li/uhfhmy
7. Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists, 68*(2), 70–77. https://dspace.mit.edu/handle/1721.1/141777
8. Tatalović, S., Grizold, A., & Cvrtila, V. (2008). Suvremene sigurnosne politike. Zagreb: Golden marketing-Tehnička knjiga. https://pdfcoffee.com/suvremene-sigurnosne-politike-pdf-free.html
9. Shaffer, G. (2012). International law and global public goods in a legal pluralist world. *The European Journal of International Law, 23*(3), 669–693. https://doi.org/10.1093/ejil/chs036
10. Maskun, S. H. (2013). Cybersecurity: Rule of use internet safely. *Journal of Law, Policy and Globalization*, (15). https://doi.org/10.1016/j.sbspro.2013.10.333